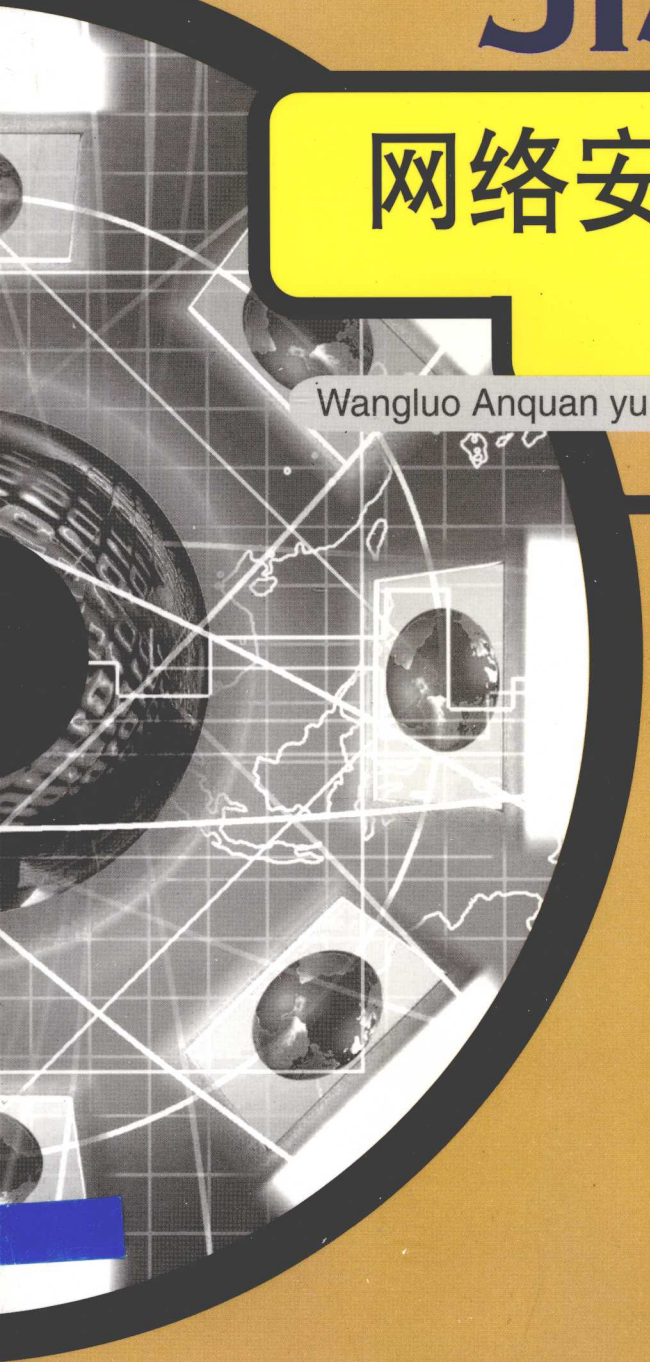
高职高专计算机系列教材

JISUANJI

网络安全与管理综合实训教程

Wangluo Anquan yu Guanli Zonghe Shixun Jiaocheng

李艇　张桓　编著



重庆大学出版社

网络安全与管理综合实训教程

李 艇 张 桓 编著

重庆大学出版社

内 容 提 要

在计算机网络发展过程中，网络管理与网络安全技术都是实践性较强的一个新的领域。本书以任务驱动的方式，使学生掌握网络安全工具和网络管理工具的使用，并能够对 Windows 平台和 Linux 平台的安全管理问题进行初步的分析和解决。通过本书的实训，读者可以具有对网络安全与管理工具的实现和实践能力。

本书适合高职高专院校计算机网络技术专业学生使用，也适合从事网络管理工作的 IT 业读者学习参考。

图书在版编目(CIP)数据

网络安全与管理综合实训教程/李艇，张桓编著. —重庆：重庆大学出版社，2004.9
(高职高专计算机系列教材)
ISBN 7-5624-3258-9

Ⅰ.网… Ⅱ.①李…②张… Ⅲ.①计算机网络—安全技术—高等学校：技术学校—教材
②计算机网络—管理—高等学校：技术学校—教材 Ⅳ.TP393.0

中国版本图书馆 CIP 数据核字(2004)第 087153 号

网络安全与管理综合实训教程

李 艇 张 桓 编著

责任编辑：曾显跃 版式设计：曾显跃
责任校对：任卓惠 责任印制：秦 梅

*

重庆大学出版社出版发行
出版人：张鸽盛
社址：重庆市沙坪坝正街 174 号重庆大学(A 区)内
邮编：400030
电话：(023)65102378 65105781
传真：(023)65103686 65105565
网址：http://www.cqup.com.cn
邮箱：fxk@cqup.com.cn (市场营销部)
全国新华书店经销
重庆邮政印务有限公司印刷

*

开本：787×1092 1/16 印张：8.75 字数：218 千
2004 年 9 月第 1 版 2004 年 9 月第 1 次印刷
印数：1—4 000
ISBN 7-5624-3258-9/TP·502 定价：13.00 元

前　言

由于计算机网络的规模越来越大，结构也越来越复杂。一个完善的网络管理系统和有效的网络安全策略是计算机网络能够可靠而稳定运行的保证，也是进行网络性能分析的依据。这就需要进一步学习如何管理计算机网络，建立一个有效的、满足要求的和安全的网络系统。

另外，信息共享与信息安全永远是互相矛盾的。而 Internet 的发展使信息安全的概念发生了根本性的变化。信息安全从单机扩展到网络连接的世界范围，同时，安全技术也得到新的发展，其内容极为丰富，是从事计算机领域的人员应该很好地掌握的一门技术。

目前，无论是企业或事业的内部网络，还是 IT 业的运营公司都迫切需要能够从事网络管理和网络安全技术的人才。开设网络管理与安全综合实训课程的目的就是让学生从实践中验证有关理论知识和技术的应用，并通过一系列的相关实训提高学生对网络管理与网络安全方面的技能和解决实际问题的能力。

本书针对高职和高专的特点组织编写，以培养网络管理与安全维护方面的应用性人才为目标。

本书分为基于 Windows 的安全实训、内部网络安全管理实训、Linux 安全实训、网络防病毒实训 4 章，选用 NetWin 2000 作为教学演示网络管理软件，并选用若干免费版的网络安全工具作为教学实训软件。读者可以通过重庆大学出版社的网站（http://www.cqup.com.cn/）下载本书所使用的实训工具及相关的辅助教学演示软件。

本书第 1 章、第 2 章、第 3 章由李艇编写，第 4 章由张桓编写，全书由李艇统编。本书经南开大学刘瑞挺教授审阅。

本书在编写过程中得到了北京华信亿码科技发展有限公司的大力支持，在此谨表衷心的感谢。

本书中的许多实验由张峰晓、李睿、臧源、王景瑞、葛亚男、尔鑫欣、张风英做了大量的基础性工作，一并表示真诚的感谢。

限于本人的学术水平，书中存在错误和不当之处难免，敬请读者批评指正。

作　者：李　艇
E-mail：litingcn@sina.com
2004 年 6 月 29 日于天津

目录

第1章 基于 Windows 的安全实训

现代计算机系统以及网络功能日渐复杂而强大，对社会各行各业产生巨大而深远的影响。同时，由于其开放性特点，使得安全问题越来越突出。所以，应该分析和研究黑客入侵技术、网络安全漏洞、数据加密技术、防火墙技术等，并通过实践体会黑客的攻击方法，掌握有效的防范技术，才能够真正的“建好网、管好网、用好网”。

通过网络安全实训将更好地理解网络安全技术与应用，有效地掌握网络安全工具的实际使用，全面提高网络安全管理技能和解决基本实际问题的能力。

1.1 探测 Internet

1.1.1 实训任务和目的

①熟练掌握 ping 应用程序，会通过 ping 目标主机，了解目标主机的一些基本信息和网络的连通情况。

②熟练掌握 tracert 应用程序，会通过 tracert，知道在本地主机和目标主机之间的路径，为进一步得到网络的拓扑结构打下基础。

③学会当网络出现问题时，用现有的网络工具去分析、发现和解决问题。

1.1.2 实训方法和步骤

(1)最常用的网络诊断工具 ping

1)ping 是一个测试程序

其执行格式如下：

ping [远程服务器名][参数]

①常用 ping 命令参数选项：

ping IP-t 连续对 IP 地址执行 ping 命令，用“Ctrl + C”中断。

ping IP-L 2000 指定 ping 命令中的数据为 2 000 字节，而不是缺省的 32 字节。

ping IP-n 执行特定次数的 ping 命令。

②如:ping 192.168.0.2 -n 2 为执行 ping 两次而不是默认的 4 次，如图 1.1 所示。

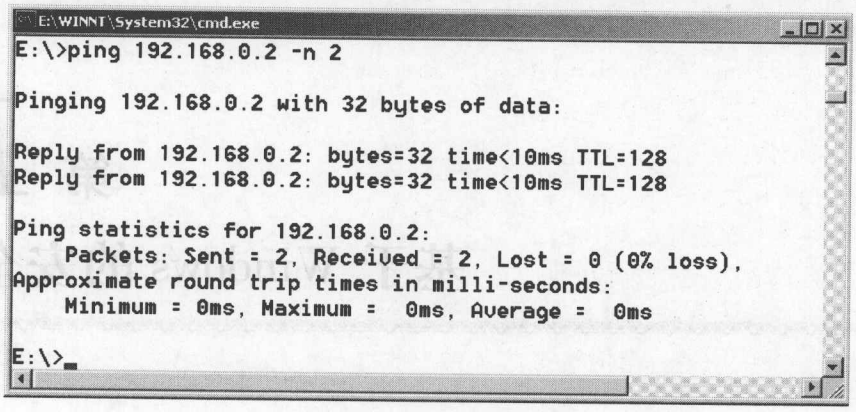


图 1.1　命令 ping 执行结果

③如:ping www. yesky. com,运行这个命令将得到天极网的 IP 地址、传送数据包的最大时间和最小时间等,如图 1.2 所示。

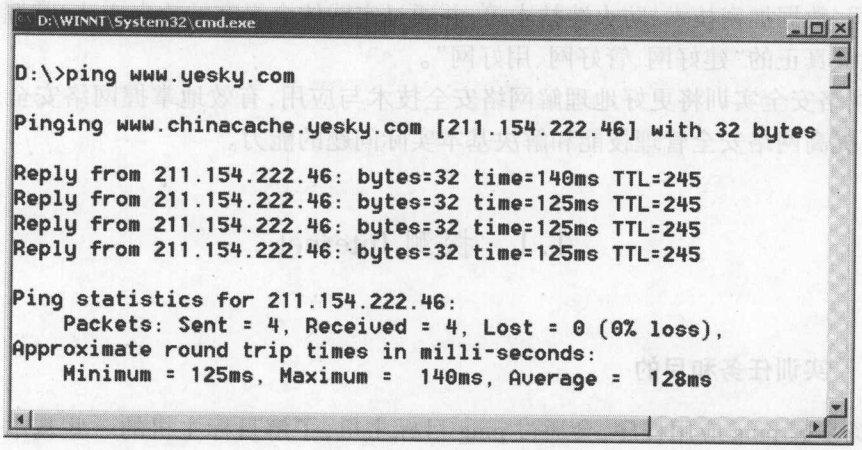


图 1.2　ping 天极网的结果

2)对屏幕出现的信息进行解释

①ping www. yesky. com [211. 154. 222. 46] with 32 bytes of data

将 32 字节数据发送到远程服务器 www. yesky. com;211. 154. 222. 46 为该服务器的 IP 地址,有时还可用其实现域名与 IP 地址的转换功能。

②Reply from 211. 154. 222. 46: bytes = 32 time = 153ms ttl = 245

本地主机已收到回送信息,具体为:32 字节,共用 140 ms,ttl 为 245。可以通过 TTL 值推算数据包已经通过了多少个路由器。源节点 TTL 起始值(就是比返回 TTL 略大的一个 2 的乘方数,如 128、256 等)减去返回时 TTL 值。例如,返回 TTL 值为 119,那么可以推算数据包离开源地址的 TTL 起始值为 128,而源地点到目标地点要通过 9 个路由器网段(128 ~ 119),如果返回 TTL 值为 245,TTL 起始值就是 256,源地点到目标地点要通过 11 个路由器网段。

③若出现 request timed out 的返回信息则为:时间超时,说明此时网络繁忙或网络不通,可以稍后再试。

④ping statistics for 211. 154. 222. 46:

Packets: Sent = 4, Received = 4, lost = 0 (0%)

Approximate round trip times in milli-seconds:

Minimum = 125 ms, Maximum = 140 ms, Average = 128 ms

ping 211.154.222.46 的信息如下：

A. 数据包个数：发送 4 个数据包(系统缺省设置)。

B. 共回收到 4 个。

C. 共丢失 0 个占总数的 0%。

D. 发送时间概括：最快回收时间 125 ms，最慢回收时间 140 ms，平均时间 128 ms。

(2)使用 tracert 命令检测路由和拓扑结构信息

网络管理员使用的另一个网络工具是 tracert. exe，用来确定去往远程目标路径上的中间计算机。

①打开“开始”-“运行”，输入 cmd，打开命令行窗口。

②输入命令：tracert 192.168.0.x (x 为合作伙伴的座位号)，观察结果如图 1.3 所示。

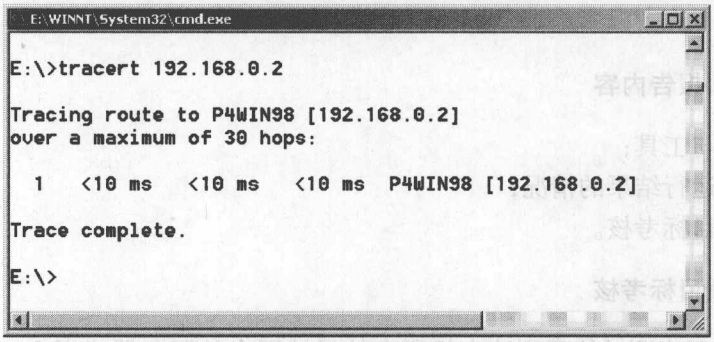


图 1.3　tracert 命令

③输入命令：tracert sina.com 回车确认，其目标路径的 IP 地址及到达时间如图 1.4 所示。

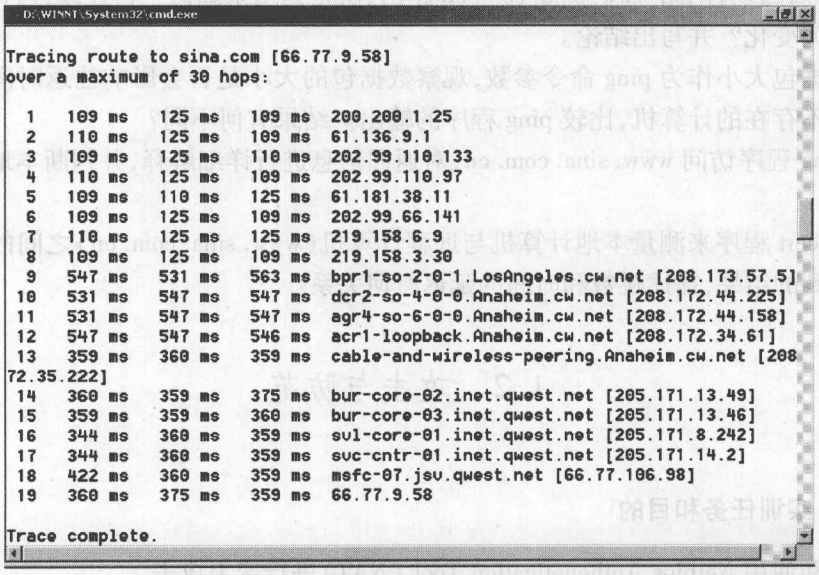


图 1.4　检测到新浪网站的路由及时间

④输入 tracert yahoo. com，回车确认，此时可观察到 tracert 没有成功检测到最终结果，如图 1.5 所示。

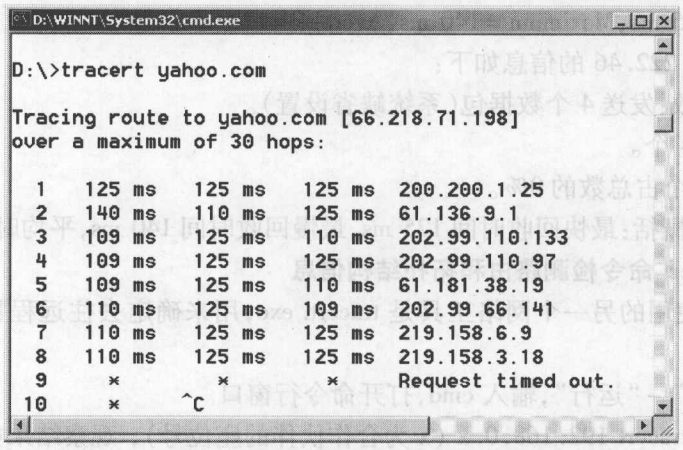


图 1.5　tracert yahoo 的结果

1.1.3　实训报告内容

①实训环境与工具；
②完成实训运行结果的情况；
③完成实训目标考核。

1.1.4　实训目标考核

①试用 ping 程序测试能否到达本机所在的局域网中的服务器或者 Internet 上的主机，并根据返回的信息查看丢失率、返回最大时间、最小时间和平均时间。

②用 tracert 查看网站 www. sina. com. cn 路由，所得到结果如何？再连续进行若干次测试，观察结果有何变化？并写出结论。

③用数据包大小作为 ping 命令参数，观察数据包的大小是否会影响往返时间。对于关闭的计算机和不存在的计算机，比较 ping 程序的输出。结果有何不同？

④用 ping 程序访问 www. sina. com. cn，对返回信息进行详细解释，并判断本地与服务器之间的跳数。

⑤用 tracert 程序来测量本地计算机与远程计算机(www. sina. com. cn)之间的跳数。比较 ping 程序得到的结果，描述跳数和时间的延迟有何关系？

1.2　攻击与防范

1.2.1　实训任务和目的

①学习和使用 Netbios Authenetication Tool (NAT)进行蛮力攻击。
②通过 NAT 了解字典攻击的原理。

③理解合理定制账号策略和强制使用强壮密码的重要性。

1.2.2　实训方法和步骤

(1)使用 NAT 进行蛮力攻击

①以 Administrator 登录系统,在“开始”—“程序”—“管理工具”—“计算机管理”中添加 testone 和 testone 两个用户,并设置密码 xx,如图 1.6 所示。

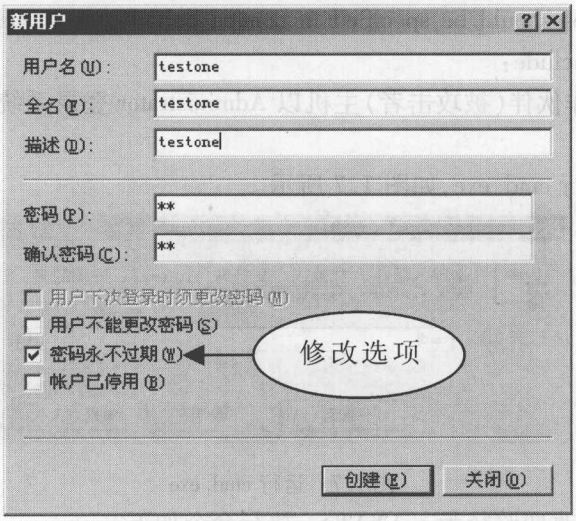


图 1.6　添加新用户

②从教师机中将 NAT 文件夹,拷贝到 c:\目录下。文件夹中各程序分别为:

nat. exe——主程序;

out. txt——运行结果的输出;

userlist. txt——用户列表,打开该文件在任意行添加 testone;

passlist. txt——密码字典文件,该文件是攻击成功的关键。在该文件中添加密码“xx”(保证实训的成功)。

③NAT 说明:

NAME

nat-NetBIOS Auditing Tool

SYNOPSIS

nat [-o < output >][-u userlist >][-p < passlist >] < address >

DESCRIPTION

nat is a tool written to perform various security checks on systems offering the NetBIOS file sharing service. nat will attempt to retrieve all information availible from the remote server, and attempt to access any services provided by the server.

OPTIONS

-o Specify the output file. All results from the scan will be written to the specified file, in addition to standard output.

-u Specify the file to read usernames from. Usernames will be read from the specified file

when attempting to guess the password on the remote server. Usernames should appear one per line in the specified file.

-p Specify the file to read passwords from. Passwords will be read from the specified file when attempting to guess the password on the remote server. Passwords should appear one per line in the specified file.

< address >

Addresses should be specified in comma deliminated format, with no spaces. Valid address specifications include:

④相邻机器或合作伙伴(被攻击者)主机以 Administrator 登录系统,并设置登录用户和密码(同第一步)。

⑤在(攻击方)运行 cmd. exe,如图 1.7 所示。

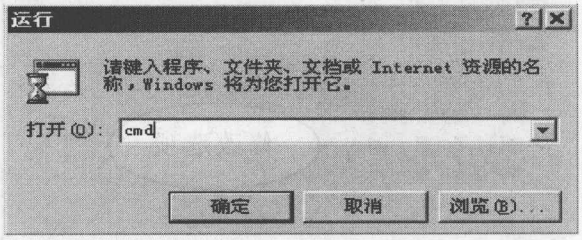


图 1.7 运行 cmd. exe

⑥在 cmd. exe 中,改变路径为 c:\NAT >,执行命令如下:

nat -o outlist. txt -u userlist. txt -p passlist. txt <合作伙伴 IP 地址如 192. 168. 0. 3 >

其中 outlist. txt 为输出文件,userlist. txt 为用户名字典,passlist. txt 为密码字典。

注意:outlist. txt 要为可读写状态,如图 1.8 所示。

图 1.8 在 cmd. exe 中运行 NAT

⑦执行以上命令行,就可以看到一系列的匹配假设,一旦获得成功,就将获得合法用户名与密码列表,如图 1.9 所示。

⑧如果在命令行中看不到提示,可打开 out. txt 文件,其中记录了所有的记录,如果匹配成功,可从中得到一些有用的信息,如图 1.10 所示。

(2)使用账号锁定策略以防范暴力攻击

①在合作伙伴机器"开始"—"程序"—"管理工具"—"本地安全策略"中选择"账户策略"下的"账户锁定策略",设置账户锁定阀值为 3,如图 1.11 所示。

图 1.9　NAT 攻击完成

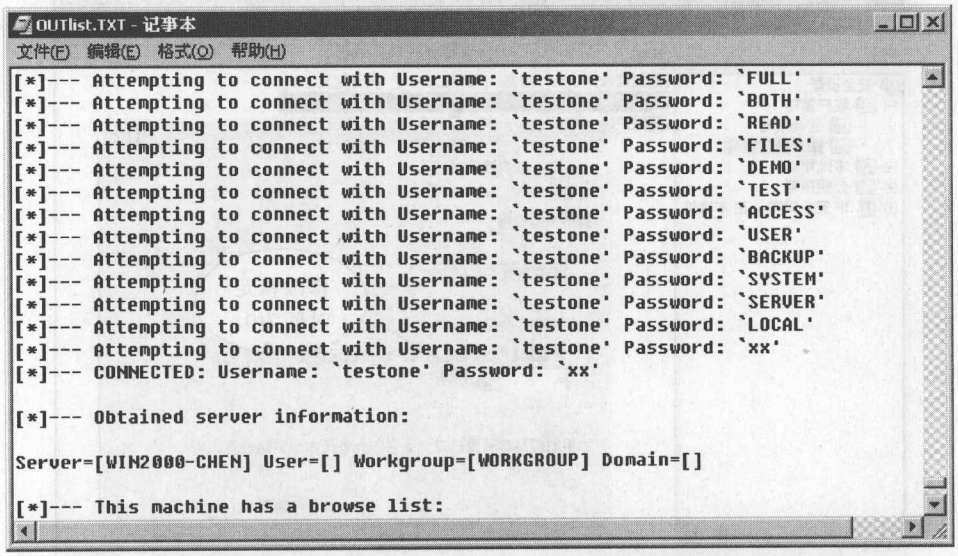


图 1.10　在 outlist. txt 中查看攻击结果

②账户锁定时间改为 0，如图 1.12 所示。

③在攻击方使用 NAT 对合作伙伴进行攻击，一系列的匹配假设之后失败，此时合作伙伴机器 testone 账户已经被锁定。

注：当账号被锁定时，再采用 NAT 这类工具进行字典攻击或暴力攻击时就不再起作用了。在使用账号锁定策略锁定的时候要仔细考虑，因黑客可以利用字典攻击的方法导致服务器上所有的账号被锁定，而不能正常地提供服务。

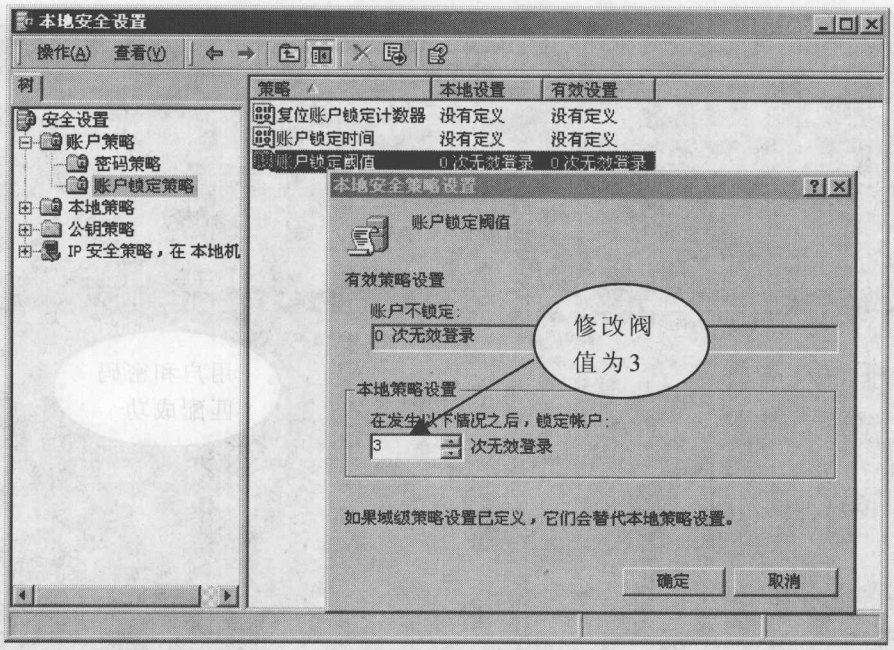


图 1.11　账户锁定阀值设置

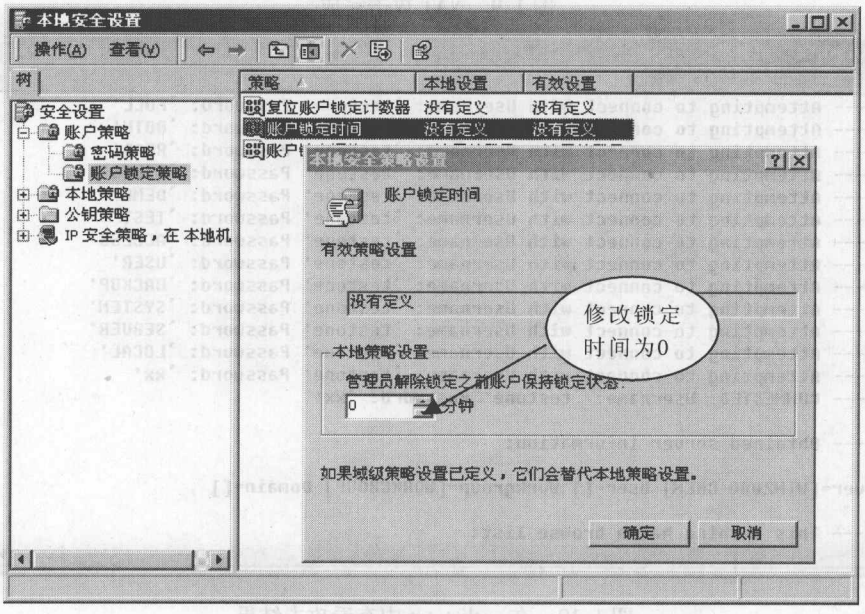


图 1.12　账户锁定时间设置

④合作伙伴注销 Administrator，重新登录，此时，先用 testone 账户登录，会弹出对话框警告此账户以锁定，再用 testtwo 账户登录，将会成功。

⑤合作伙伴登录成功之后，打开“计算机管理”，分别查看 testone 和 testtwo 账户属性，如图 1.13 所示。

在用 NAT 攻击过程中，只对 testone 进行了密码匹配，并且超过了账户锁定阀值，所以账户被锁定，登录不成功；而 testtwo 账户却没有被锁定，登录成功。

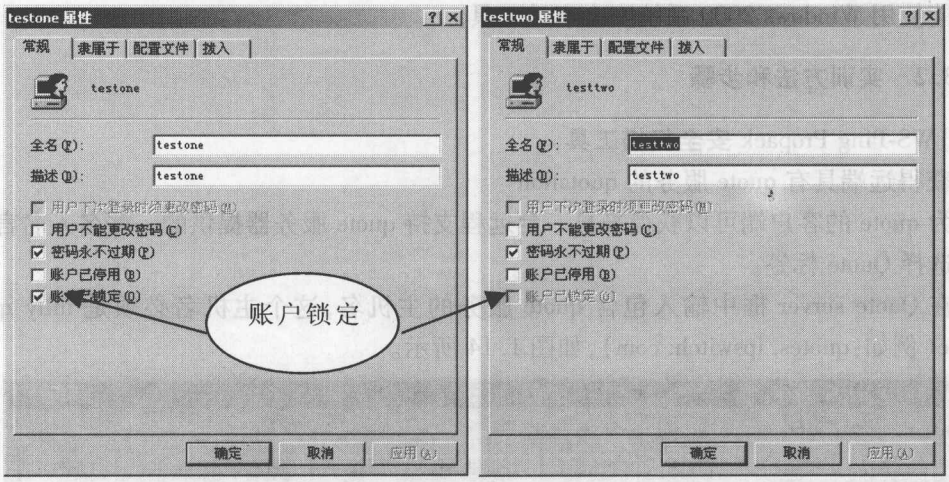


图 1.13　testone 和 testtwo 账户属性

1.2.3　实训报告内容

①实训环境与工具。

②实训运行结果。

③完成实训目标考核。

④写出实训总结及体会。

1.2.4　实训目标考核

①NAT 是一种比较古老的远程破解 NT 账号和密码的黑客工具，目前较流行的流光等软件也是根据其原理，都是利用微软的协议漏洞来进行攻击的。请问是哪个协议的漏洞，其开放的端口号是多少？

②打开 userlist. txt，在 testone 之前添加 Administrator，使用 NAT 对合作伙伴进行攻击，看有什么结果，Administrator 账户是否被锁定，重新用 Administrator 账户登录，能否成功？为什么？

③远程蛮力攻击是一种非常实际有效、目的性很强的攻击手段，它的成功与否与哪些因素有关？

④利用“本地安全设置”对密码策略进行配置，启用密码复杂性要求；密码最长存留期为 42 天；设置密码长度最小值为 8 并让合作伙伴登录。

⑤利用“本地安全设置”对账户策略进行配置，账户锁定阈值为 3 次；锁定时间为 30 min。

1.3　安全审计

1.3.1　实训任务和目的

①会使用 WS-Ping Propack 进行安全扫描。

②能使用 Windows 2000 系统安全审计工具。

1.3.2 实训方法和步骤

(1)WS-Ping Propack 安全扫描工具

1)获得远端具有 quote 服务的 quotation

作为 quote 的客户端可以获得来自一台远程支持 quote 服务器提供的一些名人名言。

①选择 Quote 标签。

②在 Quote server 框中输入包含 quote 服务的主机名,这个主机名必须是 fully qualified hostname(例如:quotes. ipswitch. com),如图 1.14 所示。

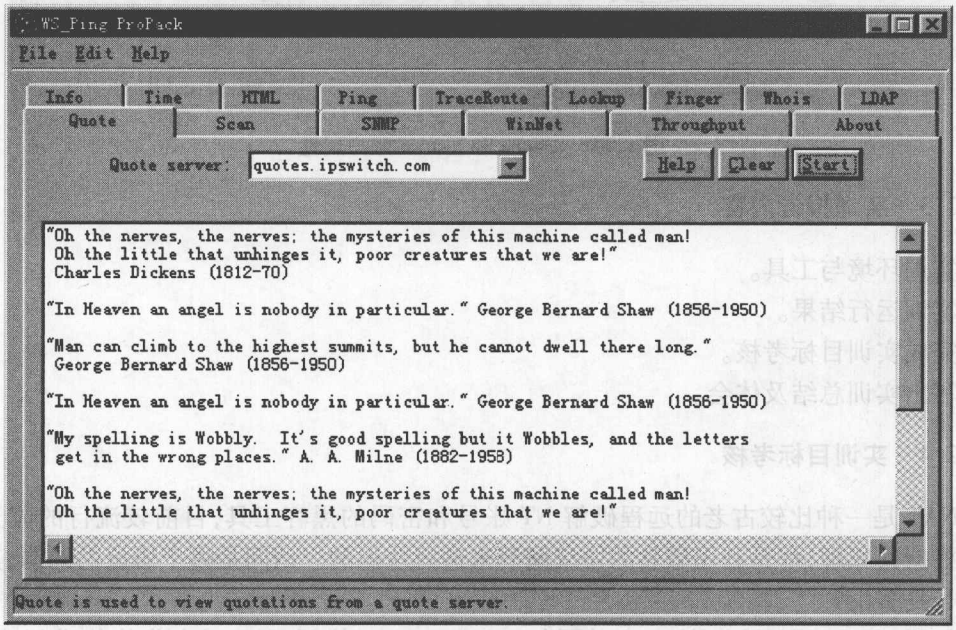


图 1.14 quotes 服务

③单击“Start”按钮。

2)显示一台主机上所有使用者的信息

finger 功能是确定和显示连接某台主机上所有用户的信息。这个信息包括显示当前用户登录该主机的用户名、主目录、登录时间、登录失败次数、最近一次收到 E-mail 的时间以及最后一次读取 E-mail 的时间。

①首先选择 finger 标签。

②在 Finger String 的文本框中输入主机名或是 IP 地址。

③单击“Start”按钮,如图 1.15 和 1.16 所示。

3)whois 命令

whois 类似于 finger 是一种 Internet 的目录服务,whois 提供了在 Internet 上某台主机或某个域的所有者的信息,如管理员姓名、通信地址、电话号码和 E-mail 地址等信息。这些信息是在官方网络 whois 服务器上注册的,如可保存在 interNIC 的数据库内。Whois 命令通常是安全审计人员了解网络情况的开始。

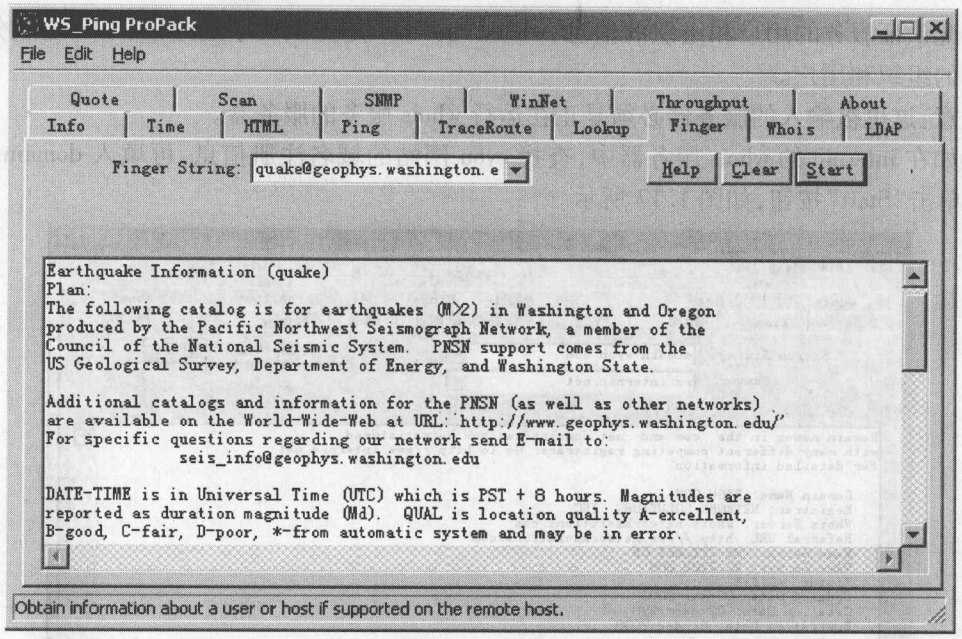


图 1.15　finger 功能

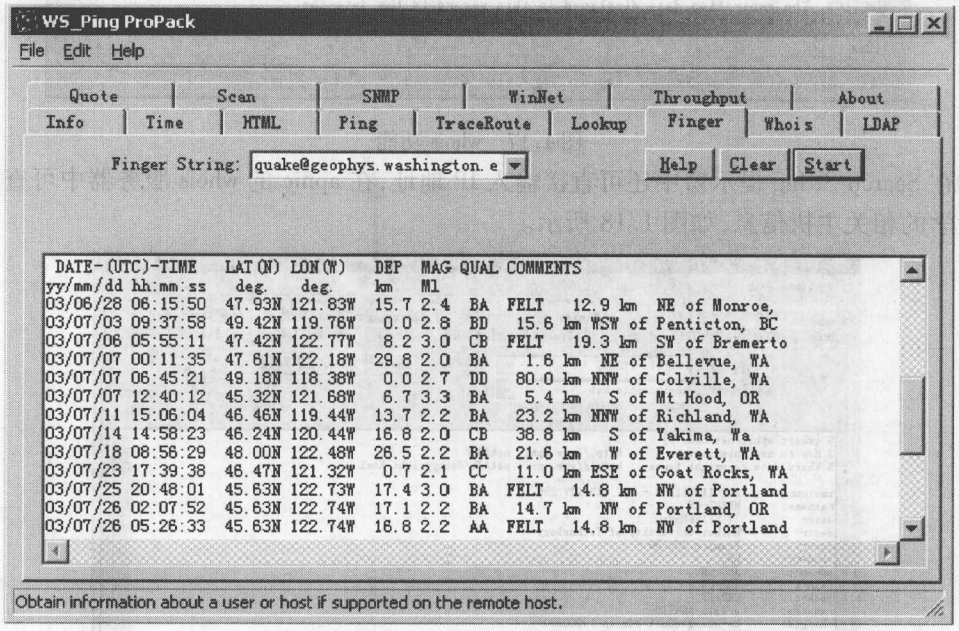


图 1.16　主机上用户信息

①打开 whois 的标签。

②如果在 Search String 中没有写上任何内容,许多 whois 服务器会返回关于如何查询其数据库的信息。

③在 Server 文本框中输入一个 whois 服务器的主机名,或是从下拉列表框中选择一个服务器。如:rs. internic. net 是提供关于用 internic 认证过的用户和组织的信息;nic. ddn. mil, whois. inc. mil 是提供有关美国军事网络用户和组织的信息;whois. arin. net 是提供经过美国 IP

地址分配认证服务的用户和组织的信息；whois. ripe. net 是提供关于通过欧洲 IP 地址分配认证服务的组织和用户。

注意：这里被输入的服务器必须是正在运行 whois 服务的服务器。

④如在 internic 的 whois 服务器中，查找 eyou 网站的域名注册信息，可填入 domain. eyou. com 后单击“Start”按钮，如图 1.17 所示。

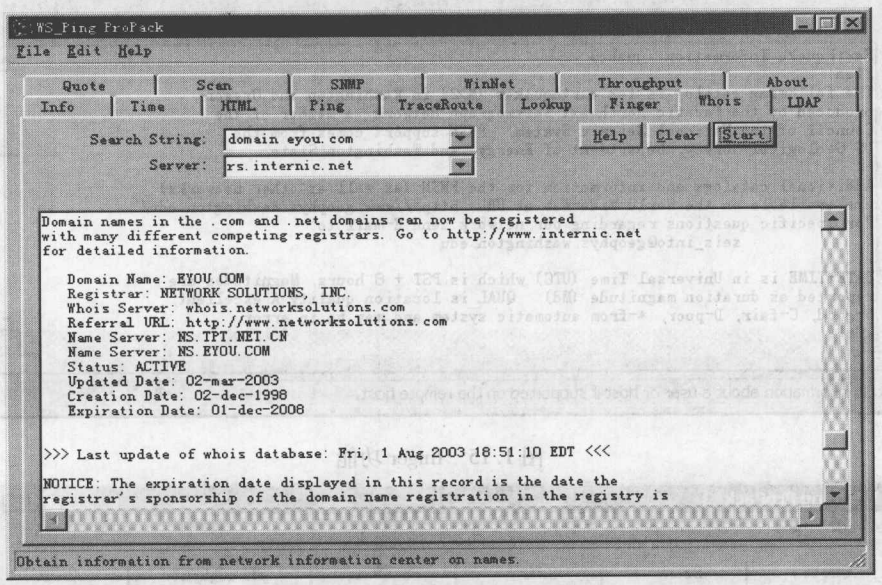


图 1.17　whois 功能

⑤在 Search String 提示窗中还可直接输入 IP 地址，在 apnic 的 whois 服务器中可查到河北工业大学的相关主机信息，如图 1.18 所示。

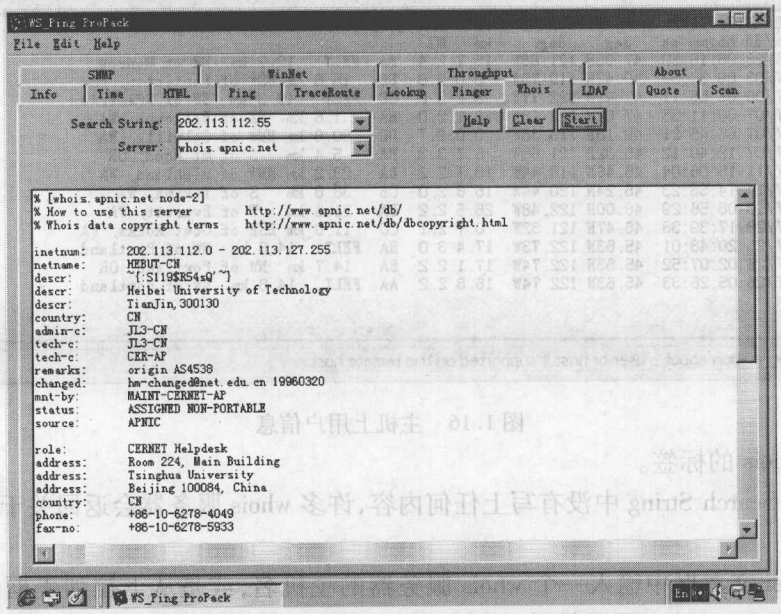


图 1.18　用户相关信息